ED480467 2003-00-00 College Student Records: Legal Issues, Privacy, and Security Concerns. ERIC Digest.

ERIC Development Team

www.eric.ed.gov

Table of Contents

If you're viewing this document online, you can click any of the topics below to link directly to that section.

ERIC Identifier: ED480467
Publication Date: 2003-00-00
Author: Holub, Tamara
Source: ERIC Clearinghouse on Higher Education Washington DC.

College Student Records: Legal Issues, Privacy, and Security Concerns. ERIC Digest.

THIS DIGEST WAS CREATED BY ERIC, THE EDUCATIONAL RESOURCES INFORMATION CENTER. FOR MORE INFORMATION ABOUT ERIC, CONTACT ACCESS ERIC 1-800-LET-ERIC

As the practice of entering student records online has become more widespread, many

colleges are struggling with the technical and legal complexities of protecting the privacy of student data. There have been a number of reports in the news of hackers breaking into college websites to steal student identifies, tamper with grades or other information, and illegally view student records. Many colleges have established policies to comply with the Family Educational Rights and Privacy Act (FERPA) of 1974, also known as the Buckley Amendment, which enumerates legal guidelines regarding the privacy of student records. However, changing technologies and the new law, the US Patriot Act, which amends some provisions of FERPA, forces colleges to reexamine how they can protect student records. This digest will briefly discuss the provisions of FERPA and the US Patriot Act, and the measures some colleges are implementing to comply with these laws and improve the security of electronic student records.

FAMILY EDUCATIONAL RIGHTS AND PRIVACY ACT (FERPA)

FERPA established specific rights to parents regarding their children's education records. These rights transfer to the student when he or she turns 18 years of age, and these students are called "eligible students" under the law. FERPA applies to educational institutions that receive federal funding. The rights established by FERPA are posted on the U.S. Department of Education website: http://www.ed.gov/offices/OM/fpco/ferpa). The basis tenants of the law state the following:
1.) Parents or eligible students have the right to inspect and review the student's education records maintained by the school, and schools are to comply with these requests.

2.) Parents or eligible students have the right to request that a school correct records which they believe to be inaccurate or misleading. If the school denies the request, the parent or eligible student is entitled to a hearing. If after the hearing, the school still denies the request, the parent or eligible student has the right to place a statement in their education records about contested information.

3.) Generally, schools must have written permission from the parent or eligible student to release information from a student's educational record. However, FERPA allows school to disclose educational records without consent to particular parties such as school officials with a legitimate educational interest.

4.) Schools may disclose, without consent, directory information such as name, address, and date of birth. However, schools must notify parents and students about directory information, and given them sufficient time to opt out of the disclosure. Finally, schools must notify parents and students annually of their rights under FERPA.

The Family Policy Compliance Office, with the U.S. Department of Education, responds

to all complaints or alleged violations under FERPA, and gives advise to colleges and schools on how to comply with the law (Walsh, 2002a). For the first time, the U.S. Supreme Court, in 2002, heard two cases based on FERPA. In February 2002, the court unanimously decided in Owasso Independent School District v. Falvo (No. 00-1073), that the practice of peer grading and students calling out each other's grades to the teacher, did not violate the provisions of FERPA (McCarthy, 2002). In Gonzaga University v. Doe (No. 01-679), the U.S. Supreme Court rules 7-2, that individuals do not have a right to sue over alleged violations under FERPA, and that individuals cannot seek compensation under that law (Walsh, 2002b). The Gonzaga ruling reaffirms the process by which the U.S. Department of Education enforces FERPA.

THE US PATRIOT ACT

As a result of the US Patriot Act, educational institutions must comply with aspects of the law that require the monitoring of foreign students and the disclosure of student records to track suspected terrorists. The US Patriot Act allows the U.S. Attorney General to access student records and collect information on foreign students, such as name, address, and visa classification which is maintained by educational institutions through the Student Exchange and Visitor Information System (SEVIS). The law also permits the U.S. Attorney General to apply for a court order to access student records maintained by educational institutions for the purpose of an investigation or prosecution relating to terrorism (American Council on Education, 2001). The law exempts both SEVIS and information obtained from student records by a court order from the disclosure clause required by FERPA. Many colleges and universities are grappling with the complexities of the law, in particular their obligations and role. A number of colleges are worried that responses to an invalid request will prompt lawsuits under the Fourth Amendment (Carlson & Foster, 2002). In response to the requirements of the law, some colleges are drafting compliance checklists for staff use to more effectively respond to law enforcement requests to search confidential university records. Librarians are concerned about privacy rights of readers since patrons' book loan records could be investigated under the U.S. Patriot Act.

ELECTRONIC SECURITY ISSUES AND COLLEGE POLICIES

Electronic information is protected not only by technology such as firewalls, password protection, and other measures, but also by the college employees who safeguard and manage the information. Some colleges have created electronic communications procedures to educate staff on how to protect student information. The University of California, Los Angeles has a policy that restricts the level of access to student information based upon what the particular staff member needs to know. For instance, academic counselors have a different level of access compared to financial aid officials. Also, before any faculty or staff member can access information, they must fill out a form detailing what they want to view and why. The form must be approved by the

computer-systems manager of the registrar's office (Foster, 2001). For computer records maintained by centers other than the registrar, U.C.L.A. gives departmental discretion to other campus managers on whether or not to retain files of websites that students visit.
Another complex issue is under what circumstances college officials have the right to view student emails or other electronic files. Many colleges reserve the right to view student emails under certain conditions. EDUCAUSE, a nonprofit association which promotes the advancement of higher education through information technology, recommends that colleges notify students about their privacy rights, have policies stating how online activity is monitored, and inform students about how their records will be used (Foster, 2001). Also, the widespread use of Social Security numbers has come under fire by those concerned with security issues. Some colleges, like the University of Illinois, are phasing out the use of Social Security numbers as student identification numbers. One college official states that the use of Social Security numbers is problematic on many campuses because many colleges do not have a disclosure policy which states how and why the college will use the information (Foster, 2002b). Under FERPA, colleges must inform students whether or not the disclosure is voluntary.

The widespread use of Social Security numbers to tract student records has made many student records vulnerable to identity theft by computer hackers or other criminals. In February 2003, hackers broke into a University of Texas database and stole the names, Social Security numbers, and email addresses of over 55,000 students and employees (''Hackers Breach Student Database at the University of Texas,'' 2003). In 2002, a Swedish hacker broke into an Indiana University database and downloaded the names and Social Security numbers of 3,100 students (Foster, 2001). In 2002, a University of Delaware student allegedly changed her grades online after successfully impersonating a professor by finding his Social Security number online and guessing the password to the professor's computer account (Read, 2002). Incidences like these often occur because software glitches or errors by university staff leave the electronic system vulnerable to attack, the lack of safeguards in protecting student information, and even organized crime rings (Foster, 2002a). Occurrences of security breaches have prompted students and some lawmakers to pressure college officials to curtail the use of Social Security numbers. Although some colleges have limited the use of students' Social Security numbers to identification purposes, many college administrators are reluctant to alter their practices, arguing that changing their procedures is too costly and time consuming and ultimately ineffective (Foster, 2002a). Laws have been passed in Arizona, California, Maryland, New York, and Wisconsin which restrict a college's use of student Social Security numbers.

CONCLUSION

The complexities of the digital age, combined with new laws designed to protect national security have altered the ways in which educational institutions provide access

to, monitor and safeguard student records. Colleges and universities have created policies tailored to the needs of their institution both to protect student records from unwanted intrusions and to comply effectively with new and complex legal and law enforcement requirements. Active debate surrounding these issues continues as educational institutions try to accommodate and balance the sometimes conflicting pressures of privacy concerns versus legal directives.

REFERENCES

American Council on Education (2001, November 5). .S. Patriot Act includes provisions on student records. Retrieved on June 24, 2003 from http://www.acenet.edu/hena/issues/2001/11-05-01/patriot.act.cfm.
Carlson, S., and Foster, A.L. (2002, March 1). Colleges Fear Anti-terrorism Law Could Turn Them into Big Brother. The Chronicle of Higher Education A31.

Foster, A.L. (2001, May 11). The Struggle to Preserve Privacy. The Chronicle of Higher Education, A37.

Foster, A.L. (2002a, August 2(. ID Theft Turns Students into Privacy Advocates. The Chronicle of Higher Education, A27, A29.

Foster, A.L. (2002b, August 2). U. of Illinois may be a model in protecting privacy. The Chronicle of Higher Education, A28.

Hackers Breach Student Database at the University of Texas (2003, March 7). Associated Press, E05.

McCarthy, M.M. (2002). The Supreme Court Addresses Student Records: Peer Grading Passes the Test. Educational Horizons, Vol. 81, Number 1, 13-15.

Read, B. (2003, august 2). Delaware Student allegedly Changed Her Grades Online. The Chronicle of Higher Education, A29.

U.S. Department of Education (2002). Family Educational Rights and Privacy Act (FERPA). Retrieved March 17, 2003 from http://www.ed.gov/offices/OM/fpco/ferpa.

Walsh, M. (2002a, April 17). Court To Decide If Pupil Privacy a Federal Case. Education Week, 25,27.

Walsh, M. (2002b, July 10). Privacy Law Not a Courtroom Matter. Justices Decide. Education Week, 35,43.

Development, under contract no. ED-99-CO-0036. The Content expressed here does not necessarily reflect the positions or policies of OERI or the Department, nor does the mention of trade names, commercial products, or organizations imply endorsement by the U.S. Government.

—

Title: College Student Records: Legal Issues, Privacy, and Security Concerns. ERIC Digest.
Document Type: Information Analyses---ERIC Information Analysis Products (IAPs) (071); Information Analyses---ERIC Digests (Selected) in Full Text (073);
Available From: ERIC Clearinghouse on Higher Education, Institute for Education Policy Studies, Graduate School of Education and Human Development, One Dupont Circle, Suite 630, Washington, DC 20036-1183. Tel: 800-956-7739 (Toll Free). For full text: http://www.eriche.org/digests/2003-1.pdf.
Descriptors: Academic Records, College Students, Confidential Records, Confidentiality, Federal Government, Federal Regulation, Foreign Students, Higher Education, Records Management, Student Records
Identifiers: ERIC Digests, Family Educational Rights and Privacy Act 1974, Student Tracking Systems